UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/974,705	10/10/2001	Marco Macchetti	01AG17653537	7872

27975 7590 05/29/2007

ALLEN, DYER, DOPPELT, MILBRATH & GILCHRIST P.A.
1401 CITRUS CENTER 255 SOUTH ORANGE AVENUE
P.O. BOX 3791
ORLANDO, FL 32802-3791

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
05/29/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/974,705	MACCHETTI ET AL.	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 February 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *21-25,27-43 and 48-51* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *21-25,27-43 and 48-51* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. In response to communications filed on 2/27/2007, applicant amends claims 21, 27-29, and 31, cancels claims 26 and 44-47 and adds claims 48-51. The following claims 21-25 and 27-43 and 48-51 are presented for examination.

1.1 In response to communications filed on 2/27/2007, the 101 rejection of claims 21-47 and the 35 U.S.C. 112, first paragraph rejection of claims 21-25 and 31-43 have been withdrawn with respect to the amendment.

1.2 Applicant's remarks, filed on 2/27/2007, with respect to the prior art rejection of claims 21-47 have been fully considered but they are not persuasive as amended. Applicant states that it appears that Luther discloses arbitrary swapping of the rows and columns of the matrix and not exchanging each of the rows with a respective column as claimed. Examiner respectfully disagrees. Luther cites, (column 5, lines 40-45 and column 5, lines 55-60 and column 6, lines 12-16)

"At step S210 the current row is initialized to the horizontal interval m. For example, as shown in FIG. 7, m is initialized to 3 and S is 1. The process then goes to step S211 via connector 301 and the data bits in the image buffer are complemented for row 3 and the successive following row 4.
At step S214 the current column is initialized to the vertical interval n. For example, as shown in FIG. 8 n is initialized to 4 and S is 1. The process proceeds to step S215 via connector 303 and the data bits in the image buffer are complemented for column 4 and the successive following column 5.

When executing steps S211 and S215 for complementing the data signals in the rows and the columns respectively, a substitution of a swap row/column or a shift row/column end around function could be implemented to further confuse the data."

As interpreted by Examiner, Luther discloses that row 3 and row 4 are being complemented as well as column 4 and column 5 in steps 211 and 215 respectively, and when executing steps 211 and 215 a substitution of a swap row/column would eventually exchange rows 3 and 4 with columns 4 and 5; this meets the recitation of exchanging each of the rows with a respective column. Applicant has amended claims 21, 27-29, and 31, and added claims 48-51. Claim limitations found previous in dependent claims 22-23 and 26 have been added to the independent claims as amended. Upon further consideration, Applicant has not overcome the rejection and the claims 21-25 and 27-43 and 48-51 remain rejected in view of Ohkuma et al and Luther.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 21-25, 27-43 and 48-51 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Publication US 2001/0024502 to **Ohkuma et al** in view of US Patent 5,533,127 to **Luther**.

As per claim 21, Ohkuma et al substantially teaches a method for converting data between an unencrypted format and an encrypted format, the data being organized in bit words, the method comprising: *converting the data by at least performing a plurality of transformation rounds* (see paragraph 92), *applying at least one transformation to a two-dimensional array of rows and columns of bit words defining a state array* (page 12, paragraphs 272-274 and figure 30); *applying at least one round key to the state array in at least one of the transformation rounds* (see **Ohkuma et al**, paragraphs 310-311 and 319). **Ohkuma et al** discloses that a matrix obtained by substituting rows and substituting columns and transposing the rows and columns in another matrix (state array) may be used (paragraph 268). As interpreted by examiner the transposing is performed by substituting rows and substituting columns to obtain a transposed MDS matrix (state array) for instance, in figure 31, to obtain y, a transformation is performed to obtain a transposed state of the matrix (paragraph 270 states executing transformation by means of a matrix) therefore, **Ohkuma et al** discloses transposing each of the *rows and columns of the state array to form a transposed state array for at least one of the transformation rounds so that at least one transformation is applied to the transposed state array* (see paragraphs 261-271 see figure 30). **Ohkuma et al** does not explicitly disclose *exchanging each row with a respective column of the state array to form a transposed state array.* **Luther** in an analogous art discloses an encryption system for two-dimensional binary data using a plurality of rounds or passes. In

each pass each row and each column of binary data is encrypted (see column 1, lines 35-39). In one exemplary embodiment, **Luther** suggests that during the process of encryption, when executing steps 211 and 215 in complementing the data signals in the rows and the columns respectively, a substitution of a swap row/column could be implemented to further confuse the data (see column 6, lines 12-16). As interpreted by Examiner, Luther discloses that row 3 and row 4 are being complemented as well as column 4 and column 5 in steps 211 and 215 respectively, and when executing steps 211 and 215 a substitution of a swap row/column would eventually exchange rows 3 and 4 with columns 4 and 5, which meets the recitation of exchanging each of the rows with a respective column. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Ohkuma et al** to perform *exchanging each row with a respective column of the state array to form a transposed state array* to further confuse the data as suggested by **Luther**. One of ordinary skill in the art would have been motivated to do so because it would add another layer of security by hiding the data used in the process of encryption therefore it would be harder for an attacker to be successful in a cryptanalysis attack since the exchanging of row/column is added to confuse the data as suggested by **Luther** (see column 6, lines 12-16).

As per claim 31, Ohkuma et al substantially teaches a device for converting data between an unencrypted format and an encrypted format, the device comprising: at least one register for storing the data in the form of bit words (see figure 10); and a circuit for *performing a plurality of transformation rounds* (see paragraph 92), *applying at least one transformation to a two-dimensional array of rows and columns of bit words defining a state array* (page 12,

paragraphs 272-274 and figure 30); *applying at least one round key to the state array in at least one of the transformation rounds* (see **Ohkuma et al**, paragraphs 310-311 and 319). **Ohkuma et al** discloses that a matrix obtained by substituting rows and substituting columns and transposing the rows and columns in another matrix (state array) may be used (paragraph 268) . As interpreted by examiner the transposing is performed by substituting rows and substituting columns to obtain a transposed MDS matrix (state array) for instance, in figure 31, to obtain y, a transformation is performed to obtain a transposed state of the matrix (paragraph 270 states executing transformation by means of a matrix) therefore, **Ohkuma et al** discloses transposing each of the *rows and columns of the state array to form a transposed state array for at least one of the transformation rounds so that at least one transformation is applied to the transposed state array* (see paragraphs 261-271 see figure 30). **Ohkuma et al** does not explicitly disclose *exchanging each row with a respective column of the state array to form a transposed state array*. **Luther** in an analogous art discloses an encryption system for two-dimensional binary data using a plurality of rounds or passes. In each pass each row and each column of binary data is encrypted (see column 1, lines 35-39). In one exemplary embodiment, **Luther** suggests that during the process of encryption, when executing steps 211 and 215 in complementing the data signals in the rows and the columns respectively, a substitution of a swap row/column could be implemented to further confuse the data (see column 6, lines 12-16). As interpreted by Examiner, Luther discloses that row 3 and row 4 are being complemented as well as column 4 and column 5 in steps 211 and 215 respectively, and when executing steps 211 and 215 a substitution of a swap row/column would eventually exchange rows 3 and 4 with columns 4 and 5, which meets the recitation of exchanging each of the rows with a respective column.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Ohkuma et al** to perform *exchanging each row with a respective column of the state array to form a transposed state array* to further confuse the data as suggested by **Luther**. One of ordinary skill in the art would have been motivated to do so because it would add another layer of security by hiding the data used in the process of encryption therefore it would be harder for an attacker to be successful in a cryptanalysis attack since the exchanging of row/column is added to confuse the data as suggested by **Luther** (see column 6, lines 12-16).

As per claims 22 and **32**, the references as combined above disclose the limitation of *wherein said at least one register stores bit words as 8-bit words* (**Ohkuma et al**, page 6, paragraph 128).

As per claims 23 and **33**, the references as combined above disclose the limitation of *wherein said circuit operates on a state array comprising a 4x4 matrix of bit words* (**Ohkuma et al**, page 6, paragraph 128).

As per claims 24 and **34**, the references as combined above disclose *said circuit in performing a plurality of transformation rounds performs at least 10 transformation rounds* (**Ohkuma et al**, page 4, paragraph 92).

As per claim 25, the references as combined above disclose *performing at least one* stage or *round on a non-transposed matrix* (state array); (see **Ohkuma et al**, paragraph 241) stating "the final round does not include any higher-level MDS". Performing at least one round on a non-transposed state array is well known as disclosed in Rijndael cipher algorithm. (See also **Ohkuma et al**, page 4, paragraph 87, and prior art figure 4 of Applicant's disclosure).

As per claim 27, the references as combined above disclose the limitation of *wherein the at least one round key is transposed* (see **Ohkuma et al**, figure 3 and figure 6 and page 5, paragraph 109).

As per claim 28 the references as combined above disclose the limitation of *adding code to transpose the at least one round key* (see **Ohkuma et al**, page 6, paragraphs 140-142; see also page 7, paragraph 147).

As per claim 29, the references as combined above disclose the limitation of *wherein the at least one round key comprises a plurality of round keys, each corresponding to a respective transformation round and being applied according to a round key schedule* (see **Ohkuma et al**, page 7, paragraph 147).

As per claim 30, the references as combined above disclose the limitation of wherein the *round key schedule comprises a transposed round key schedule* (see **Ohkuma et al**, page 7, paragraph 147). The transformation applied to the round key schedule by diffusing random keys

and applied different constants at different units of rounds meets the recitation of a transposed round key schedule.

As per claim 35, the references as combined above disclose *wherein said circuit comprises at least one S-box processing module, said at least one S-box processing module operating on a group of bit words defining a cell of a column of the state array* (see **Ohkuma et al**, figure 6, 112).

As per claim 36, the references as combined above disclose *wherein the at least one S-box processing module comprises a plurality of S-box modules, each of the plurality of S-box modules operating on a corresponding cell of a column of the state array* (see **Ohkuma et al**, figure 6, 112).

As per claim 37, the references as combined above disclose the limitation of *wherein the column of the state array comprises four cells* (**Ohkuma et al**, page 4, paragraph 92).

As per claims 38-39, the references as combined above disclose that the invention can be performed by any number of modules and any combination of bits wherein the circuit further comprises a plurality of shift column modules, (**Ohkuma et al**, page 3, paragraphs 62-65); and further discloses shift up can be performed (**Ohkuma et al**, page 5, paragraph 117); column mix is also a well known process as disclosed in Rijndael cipher algorithm (**Ohkuma et al**, page 1, paragraph 5 and page 4, paragraph 87) that meets the recitation of *each of said plurality of shift*

column modules to perform a column shift operation on a column of the state array and the limitation of *wherein a column shift operation performed by each of said plurality of shift column modules generates shift column data, and wherein said circuit further comprises a single mix column module to perform column mix operations on shift column data.*

As per claims 40-43, the references as combined above disclose an encryption and decryption apparatus that meets the recitation of *encoder* for converting data from an unencrypted data format to an encrypted data format and a *decoder* for converting data from an encrypted data format to an unencrypted data format (**Ohkuma et al**, page 15, paragraph 343-349). **Ohkuma et al** further discloses an encryption and decryption apparatus formed as a semiconductor device that meets the recitation of *embedded system for use in a smart card* (**Ohkuma et al**, page 15, paragraph 343-349).

As per claim 48, **Ohkuma et al** substantially teaches a method for converting data between an unencrypted format and an encrypted format, the data being organized in bit words, the method comprising: *converting the data by at least performing a plurality of transformation rounds for converting the data* (see paragraph 92) comprising, *applying at least one transformation to a two-dimensional array of rows and columns of 8-bit words defining a state array* (page 12, paragraphs 272-274 and figure 30) comprising a *4x4 matrix of bit words* (**Ohkuma et al**, page 6, paragraph 128); *applying at least one round key to the state array in at least one of the transformation rounds* (see **Ohkuma et al**, paragraphs 310-311 and 319). **Ohkuma et al** discloses that a matrix obtained by substituting rows and substituting columns and

transposing the rows and columns in another matrix (state array) may be used (paragraph 268). As interpreted by examiner the transposing is performed by substituting rows and substituting columns to obtain a transposed MDS matrix (state array) for instance, in figure 31, to obtain y, a transformation is performed to obtain a transposed state of the matrix (paragraph 270 states executing transformation by means of a matrix) therefore, **Ohkuma et al** discloses transposing each of the *rows and columns of the state array to form a transposed state array for at least one of the transformation rounds so that at least one transformation is applied to the transposed state array* (see paragraphs 261-271 see figure 30). **Ohkuma et al** does not explicitly disclose *exchanging each row with a respective column of the state array to form a transposed state array*. **Luther** in an analogous art discloses an encryption system for two-dimensional binary data using a plurality of rounds or passes. In each pass each row and each column of binary data is encrypted (see column 1, lines 35-39). In one exemplary embodiment, **Luther** suggests that during the process of encryption, when executing steps 211 and 215 in complementing the data signals in the rows and the columns respectively, a substitution of a swap row/column could be implemented to further confuse the data (see column 6, lines 12-16). As interpreted by Examiner, Luther discloses that row 3 and row 4 are being complemented as well as column 4 and column 5 in steps 211 and 215 respectively, and when executing steps 211 and 215 a substitution of a swap row/column would eventually exchange rows 3 and 4 with columns 4 and 5, which meets the recitation of exchanging each of the rows with a respective column. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Ohkuma et al** to perform *exchanging each row with a respective column of the state array to form a transposed state array* to further confuse the data

as suggested by **Luther**. One of ordinary skill in the art would have been motivated to do so because it would add another layer of security by hiding the data used in the process of encryption therefore it would be harder for an attacker to be successful in a cryptanalysis attack since the exchanging of row/column is added to confuse the data as suggested by **Luther** (see column 6, lines 12-16).

As per claim 49, the references as combined above disclose the limitation of *wherein the at least one round key is transposed before being applied to the state array* (see **Ohkuma et al**, figure 3 and figure 6 and page 5, paragraph 109).

As per claim 50 the references as combined above disclose the limitation of *adding code to transpose the at least one round key* (see **Ohkuma et al**, page 6, paragraphs 140-142; see also page 7, paragraph 147).

As per claim 51, the references as combined above disclose the limitation of *wherein the at least one round key comprises a plurality of round keys, each corresponding to a respective transformation round and being applied according to a round key schedule* (see **Ohkuma et al**, page 7, paragraph 147).

Conclusion

3. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

3.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on 8:00-6:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from

a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

cc

Carl Colin

Patent Examiner

May 15, 2007

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER